

# Web-Security - Mediawiki

Hardening Mediawiki

---

Konzeption und Implementierung einer  
Sicherheitsarchitektur

# Web-Security - Mediawiki

## Das Team:

- Patrick Schneider
- Eric Hartmann
- Björn Rathjens
- Christopher Allan
- Tobias Homberg
- Mark Schlüter
- Thomas Kraebihl
- Dieter Kramer

# Web-Security - Mediawiki

- Ermittelter Schutzbedarf des Zielsystems
  - niedrig bis mittel
- Integration von PHPIDS in Mediawiki
- PHPIDS als Extension zu Mediawiki
- Adminseite zur Konfiguration von PHPIDS
- URL zum Testsystem:
  - <https://hardening-mediawiki/index.php/Hauptseite>
- Zugangsdaten: HMW / WebSec2010

# Web-Security - Mediawiki

spezialseite

## PHPIDS Administration

MediaWiki.Care  
"Where your Wiki is safe"

PHPIDS Manager

Verwaltung Rules Impactlogs Stats

Verwaltung

Status ☒ on ☐ off

Filtertyp

Basispfad

Empfänger

Filterpfad

tmp pfad


Keys prüfen? ☒ false ☐ true

Senden Reset

- Administration
- Verwaltung durch den PHPIDS Manager
  - Rules
  - Impactlogs
  - Stats
- PHPIDS kann Ein bzw. Ausgeschaltet werden
- Angabe der E-Mailadresse für die Benachrichtigung bei einem Hackerangriff

# Web-Security - Mediawiki

# PHPIDS Administration



MediaWiki.Care  
"Where your Wiki is safe"

## PHPIDS Manager

Verwaltung
Rules
Impactlogs
Stats

## PHPIDS Rules

id	Regel	Beschreibung	Tags	Impact
1	<code>(?:[^\"]*["?&gt;] (?:[^\w\s]*V&gt;))(?:&gt;")</code> finds html breaking injections including whitespace attacks	xss, csrf,	4	
2	<code>(?:'+.*[=]"[^\"]*" )(?:'\w+\s*=) (?:&gt;\w=V) (?:#.+)[\s"&gt;] (?:'\s*(?:src style on w</code> finds attribute breaking injections including whitespace attacks	xss, csrf,	4	
69	<code>(?:[\s'dV"]+(?:on w+style poster background)=[\s\w])</code> finds malicious attribute injection attempts	xss, csrf,	6	
3	<code>(?:^&gt;[\w\s]*&lt;V?\w{2,}&gt;)</code> finds unquoted attribute breaking injections	xss, csrf,	2	
4	<code>(?:[+V]\s*name[\W\d]*[+]) (?:\W*url\s*=\) (?:[^\w\sV?&gt;]\s*(?:location referrer nar</code> Detects url-, name-, JSON, and referrer-contained payload attacks	xss, csrf,	5	
5	<code>(?:\W\s*hash\s*[^\w\s-]) (?:\w+=\W*["'*,.[^\s(){} (?:\?["'"])*](?:&lt;!\V)__[a-z</code> Detects hash-contained xss payload attacks, setter usage and property overloadin	xss, csrf,	5	

- PHPIDS Rules
- Auflistung aller möglichen Regeln
  - Regel
  - Beschreibung
  - Klasse
  - Impact
- Ändern oder Einfügen von Regeln
- Regeln werden in XML-File gespeichert

# Web-Security - Mediawiki

- Impacts
  - Angriffsvektor
  - Impact-Wert
  - Name der betroffenen Benutzervariable
  - Wert der als Angriff erkannten Benutzervariable
  - Die aufgerufene Seite
  - IP-Adresse des (vermeintlichen) Angreifers
  - Zeitpunkt der Anfrage

PHPIDS Administration

MediaWiki.Care  
"Where your Wiki is safe"

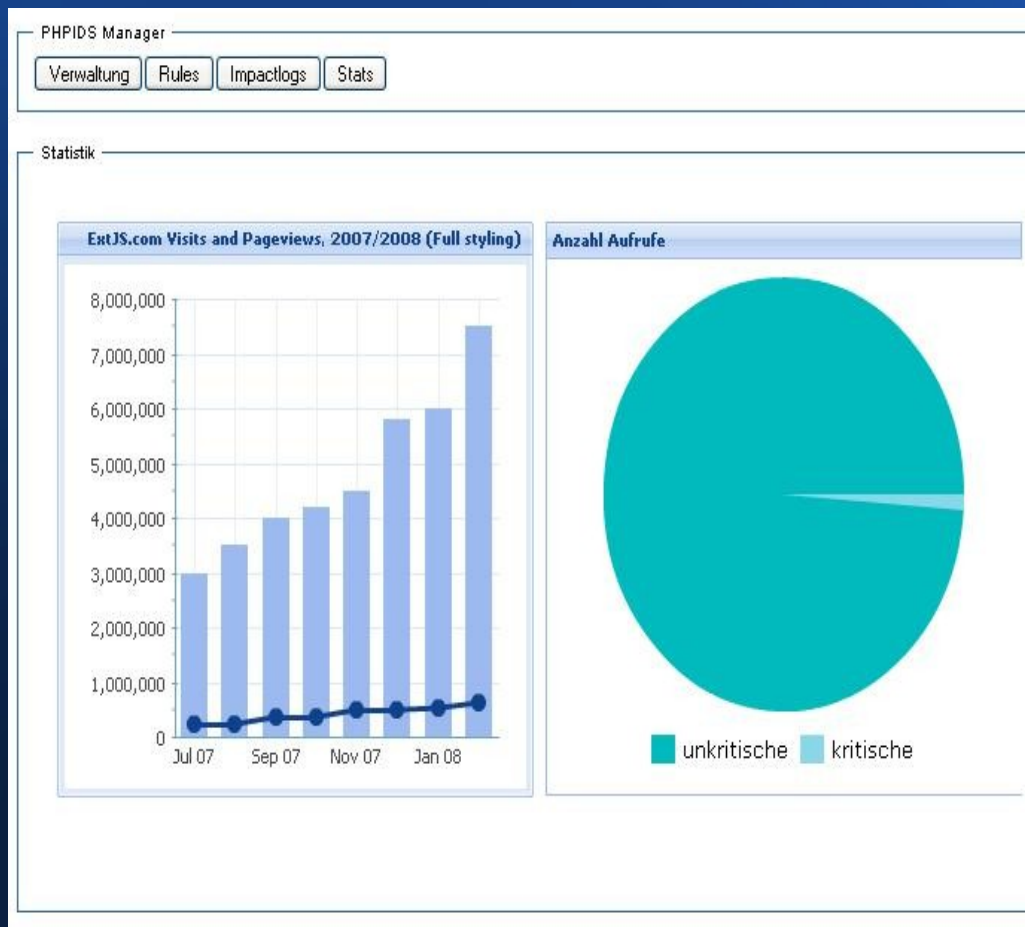
PHPIDS Manager

Verwaltung Rules Impactlogs Stats

Impacts

id	name	value	page	tags	ip	impact	origin	created
----	------	-------	------	------	----	--------	--------	---------

# Web-Security - Mediawiki



- Statistik
- Ergebnisdarstellung der statistischen Auswertung.
- Für die Erstellung der Grafiken verwenden wir das Framework Ext JS (Cross-Browser Rich Internet Application Framework)
- Anzahl der Zugriffe pro Monat
- Prozentuale Darstellung kritische / unkritische Zugriffe über einen bestimmten Zeitraum
- Weitere Auswertung möglich